REMARKS

This application has been carefully reviewed in light of the Office Action dated March 19, 2004. Claims 1 to 21 are now pending in the application, with Claims 22 to 29 having been cancelled. Claims 1, 11, and 12 are the independent claims herein. Reconsideration and further examination are respectfully requested.

Claims 1, 3, 5 to 7, and 13 to 21 were rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 6,543,052 (Ogasawara) in view of U.S. Patent No. 6,327,660 (Patel, Jr. et al.), and Claims 2, 4, and 8 to 12 were rejected under § 103(a) over Ogasawara in view of Patel and further in view of U.S. Patent No. 6,385,655 (Smith et al.). Reconsideration and withdrawal of the rejections are respectfully requested.

The present invention as recited by Claim 1 relates to printing between a client application and an interface device over secure communication paths. According to the invention, a determination is made whether a first secure communication path is established between the client application and a cable head end, and whether a second secure communication path is established between the cable head end and the interface device. In response to the determination that the first and second secure communication paths are established, print data generated by the client application is transmitted by the client application to the interface device, whereby the print data is sent to a printer attached to the interface device for printing.

With specific reference to claims, amended independent Claim 1 is a method for the secure printing of print data from a client application residing on a data network to an interface device which has a printer, the interface device residing on a digital cable network which has a cable head end for interfacing the digital cable network to the

data network, the method comprising the steps of generating print data in the client application; determining whether a first secure communication path is established between the client application and the cable head end, and whether a second secure communication path is established between the cable head end and the interface device, and transmitting, in response to a determination that the first and second secure communication paths are established, the print data from the client application to the interface device, wherein the print data is sent to the printer from the interface device for printing.

The applied art is not seen to disclose or to suggest the features of independent Claim 1. In particular, the applied art is not seen to disclose or to suggest at least the feature of determining whether a first secure communication path is established between a client application and a cable head end, and whether a second communication path is established between the cable head end and an interface device, and in response to the determination, transmitting print data generated by the client application to the interface device, whereby the print data is sent to a printer attached to the interface device for printing.

Ogasawara is seen to relate to an Internet-based electronic shopping system hosted on a television set-top box (STB) through which a user may purchase items on the Internet using features such as voice and bar code recognition built into a remote control unit. (Ogasawara, abstract; column 4, lines 24 to 34; column 7, lines 10 to 12). As admitted in the Office Action, Ogasawara fails to disclose determining whether a first secure communication path is established between a client application and a cable head end, and whether a second secure communication path is established between the cable

head end and an interface device. Thus, Ogasawara is not seen to disclose or to suggest the foregoing features of Claim 1.

It is also noted that the Office Action alleges that column 3, lines 14 to 23 of Ogasawara discloses "generating print data in a client application," and that column 5, lines 53 to 65 discloses "transmitting, in response to a determination that said secure communication path exists, said print data from said client application to said interface device." However, Applicants fail to understand these allegations. More particularly, column 3, lines 14 to 23 of Ogasawara states:

> The STB is configured to provide a user with Internet access in a manner such as currently provided by Web TV and further includes purpose-type application software such as voice recognition software and bar code recognition software to support an electronic shopping system. Application programs are either hosted on and loaded from a mass storage media such as a hard disk drive or are downloaded from an external server via a telephone modem connection, a cable or satellite connection and/or wireless broadcast means.

As is readily apparent from the foregoing description, there simply is no reference whatsoever to generating print data. Accordingly, Applicants fail to see how the foregoing section of Ogasawara allegedly discloses the claimed step of the client application generating print data as alleged in the Office Action.

Regarding the claimed step of transmitting, in response to a determination that the secure communication paths exist, the print data generated by the client application to the interface device, column 5, lines 53 to 65 of Ogasawara states:

> The data is then sent to a channel decoder 52 for decoding and extracting the data received for a particular medium. In the illustrated embodiment, the remote control unit 14 is equipped to receive voice data from the STB 10. The voice data, once extracted by the channel decoder 52, is transmitted to a digital to analog converter 54 and the converted

> analog voice data is sent to the speaker for generating corresponding sound waves to the user. It should be appreciated by those having skill in the art, that necessary variations can be made to the remote control unit without departing from the spirit and scope of the invention should other types of data other than voice data be sent by the STB 10 to the remote control unit 14.

Again, as can readily be seen, nothing in the foregoing section of Ogasawara discloses transmitting print data from a client application to an interface device, much less that the transmission is performed when a determination is made that the secure communication paths exist. Moreover, the allegation at page 4, lines 1 to 3 of the Office Action that Ogasawara discloses the foregoing feature is at odds with the Office Action's admission at page 4, lines 6 to 8 that Ogasawara fails to disclose determining whether a secure communication path exists. Thus, Applicants fail to understand how the cited portions of Ogasawara could be found to disclose the features of the present invention.

Turning now to Patel, is not seen to remedy the foregoing deficiencies of Ogasawara. In this regard, Patel is merely seen to make separate, secure connections between different devices when one device is to communicate with another device. As Applicants understand Patel, if communication were to occur between three different devices, where, for example, data is to be transmitted from device A to device B and then from device B to device C, a secure connection would be established between device A and device B, with the data being communicated from device A to device B. Then, a secure connection would be made between device B and device C, with the data being transmitted from device B to device C. Thus, in Patel, when the data is transmitted, only one secure connection is made in the communication path for transmitting the data. In contrast, in the present invention, a determination is made whether the first and second secure

communication paths are established, and once they are, the print data is transmitted via the two secure paths from a client application to an interface device. Thus, Patel is simply different from transmitting print data from a client application to an interface device once a determination has been made that a first secure communication path is established between the client application and a cable head end, and that a second communication path is established between the cable head end and the interface device.

Smith has been studied but is not seen to add anything that, when combined with Ogasawara and Patel, would have resulted in the present invention. More particularly, any permissible combination of Ogasawara, Patel and Smith is not seen to disclose or to suggest at least the feature of determining whether a first secure communication path is established between a client application and a cable head end, and whether a second communication path is established between the cable head end and an interface device, and in response to the determination, transmitting print data generated by the client application to the interface device, whereby the print data is sent to a printer attached to the interface device for printing.

In view of the foregoing deficiencies of the applied art, amended independent Claim 1, as well as the claims dependent therefrom, are believed to be allowable.

Referring now to Claim 11, similar features as claimed in Claim 1 are contained therein and therefore, Claim 11 is believed to be allowable for the same reasons as set forth above. However, Claim 11 also includes additional features which are not believed to be disclosed or suggested by the applied art. More particularly, Claim 11 includes the feature of, in response to a determination that a first secure communication

path is established between a client application and a cable head end, sending print data in a device-independent format from the client application to the cable head end, whereby the cable head end transforms the device-independent print data into a rasterized format corresponding to a printer attached to an interface device, and then, once a determination has been made that a second secure communication path is established between the cable head end and the interface device, the cable head end sends the rasterized print data to the interface device for printing. Thus, in addition to the features described above with regard to Claim 1, the applied art is not seen to disclose or to suggest at least the foregoing features of Claim 11.

The Office Action admits that both Ogasawara and Patel fail to disclose the foregoing features, but cites Smith (in relation to Claim 4) as allegedly making up for Ogasawara's and Patel's deficiencies. In this regard, the Office Action alleges that Smith uses "certificate authentication for determining a secure communication (column 20, lines 41-49) and device (platform) independent formatted document such as HTML and PDF (column 4, lines 65-67 and column 5, lines 1-11)." As Applicants understand the foregoing, the Office Action is merely asserting that Smith teaches the use of device-independent formatted documents, but Applicants fail to see any allegation that the alleged device (platform) independent documents are sent to a cable head end, whereby the cable head end transforms the device-independent formatted document into a rasterized format corresponding to a printer attached to an interface device, and the cable head end then sends the rasterized print data to an interface device. Thus, the Office Action more or less admits that Ogasawara and Smith fail to disclose or to suggest at least the feature of sending print data in a device-independent format from a client application to a cable head end,

transforming, in the cable head end, the print data into a rasterized format corresponding to a printer attached to an interface device, and sending the print data in rasterized format from the cable head end to the interface device for printing.

In view of the foregoing, amended independent Claim 11, as well as the claims dependent therefrom, are believed to allowable.

Referring now to Claim 12, device-independent format print data is transformed in a client application into a rasterized format in accordance with a printer driver corresponding to a printer attached to an interface device. The rasterized print data is then encrypted in the client application, with the encrypted print data being sent from the client application to a cable head end, and from the cable head end to an interface device, where the encrypted rasterized print data is decrypted for printing by a printer attached to the interface device. As a result, secure printing between a client application, a cable head end, and an interface device having a printer attached thereto can be accomplished by encryption of the rasterized print data.

Referring specifically to the claims, amended independent Claim 12 is a method for the secure printing of print data from a client application residing on a data network to an interface device which has a printer, the interface device residing on a digital cable network which has a cable head end for interfacing the digital cable network to the data network, the method comprising the steps of generating print data in the client application, transforming, in the client application, the print data from a device-independent format to a rasterized format in accordance with a printer driver corresponding to the printer attached to the interface device, encrypting, in the client application, the print data in the rasterized format, sending the encrypted print data in the rasterized format from the

client application to the cable head end, sending the encrypted print data in the rasterized format from the cable head end to the interface device, and decrypting, in the interface device, the print data in the rasterized format for printing by the printer.

The applied art, alone or in any permissible combination, is not seen to disclose or to suggest the features of amended independent Claim 12. In particular, the applied art is not seen to disclose or to suggest at least the feature of transforming, in a client application, print data from a device-independent format to a rasterized format in accordance with a printer driver corresponding to a printer attached to an interface device, encrypting the rasterized print data in the client application, sending the encrypted print data from the client application to a cable head end, sending the encrypted print data from the cable head end to the interface device, and decrypting the print data in the rasterized format by the interface device for printing.

As it relates to Claim 12, the Office Action admits that Ogasawara fails to disclose the foregoing features, but cites Patel's column 5, lines 34-45 and column 6, lines 1-15 as allegedly making up for the deficiencies of Ogasawara.

As Applicants understand these portions of Patel, they merely disclose a method of encrypting and decrypting data packets when data is to be transmitted between two devices. However, in the context of the claimed invention (i.e., printing from a client application to a cable head end to an interface device to a printer attached to the interface device), Patel is not seen to add anything that, when combined with Ogasawara, would have resulted in the present invention, and in particular, that would have disclosed or suggested at least the feature of transforming, in a client application, print data from a device-independent format to a rasterized format in accordance with a printer driver corresponding

to a printer attached to an interface device, encrypting the rasterized print data in the client application, sending the encrypted print data from the client application to a cable head end, sending the encrypted print data from the cable head end to the interface device, and decrypting the print data in the rasterized format by the interface device for printing.

Moreover, it is hereby submitted that, at best, a combination of Ogasawara and Patel would have resulted in the HTML web page for home shopping being encrypted before it is downloaded to the set-top box, with the set-top box then decrypting the home shopping web page for display on the television. However, Applicants fail to see any good reason why it would be necessary or even useful to encrypt an HTML web page for home shopping when it is downloaded, particularly in the context of performing home shopping via a publicly accessible web site. Thus, it is not seen why one skilled in the art would have been motivated to apply Patel's encrypted data packets to the home shopping HTML web pages of Ogasawara.

Smith has been studied but is also not seen to disclose or to suggest at least the feature of at least the feature of transforming, in a client application, print data from a device-independent format to a rasterized format in accordance with a printer driver corresponding to a printer attached to an interface device, encrypting the rasterized print data in the client application, sending the encrypted print data from the client application to a cable head end, sending the encrypted print data from the cable head end to the interface device, and decrypting the print data in the rasterized format by the interface device for printing.

In view of foregoing deficiencies of the applied art, amended independent Claim 12, as well as the claims dependent therefrom, are believed to be allowable.

No other matters having been raised, it is believed that the entire application is fully in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience.

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Supplemental to the Information Disclosure Statement dated March 22, 2004, which apparently crossed in the mail with the March 19, 2004 Office Action, Applicants wish to merely point out that each item of information cited in that Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of that Information Disclosure Statement. Accordingly, the information cited therein is deemed to have been timely submitted under 37 C.F.R. § 1.97(c) and consideration thereof is respectfully requested.

Applicants' undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicants
Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 82560v1